

IN THE CLAIMS

1. (Currently Amended) A method of detecting malicious content comprising:
 examining at least two different corresponding characteristics of a digital object;
 analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and
 upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.
2. (Original) A method for detecting malicious content according to claim 1 and wherein said malicious content comprises malicious code.
3. (Original) A method for detecting malicious content according to claim 1 and wherein said malicious content comprises masqueraded content.
4. (Original) A method for detecting malicious content according to claim 1 and wherein at least one of said at least two characteristics is selected from a set consisting of:
 header information;
 file content;
 file name extension; and
 file icon.
5. (Original) A method for detecting malicious content according to claim 4 and wherein said malicious content comprises malicious code.
6. (Original) A method for detecting malicious content according to claim 4 and wherein said malicious content comprises masqueraded content.
7. (Original) A method for detecting malicious content according to claim 1 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

8. (Original) A method for detecting malicious content according to claim 7 and wherein said malicious content comprises malicious code.

9. (Original) A method for detecting malicious content according to claim 7 and wherein said malicious content comprises masqueraded content.

10. (Original) A method for detecting malicious content according to claim 7 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

11. (Original) A method for detecting malicious content according to claim 10 and wherein said malicious content comprises malicious code.

12. (Original) A method for detecting malicious content according to claim 10 and wherein said malicious content comprises masqueraded content.

13. (Original) A method for detecting malicious content according to claim 1 and wherein said digital object comprises a file.

14. (Original) A method for detecting malicious content according to claim 1 and wherein said digital object comprises an e-mail attachment.

15. (Original) A method for detecting malicious content according to claim 1 and wherein said digital object comprises a web page.

16. (Original) A method for detecting malicious content according to claim 1 and wherein said digital object comprises a storage medium.

17. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and
file content.

18. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and
file name extension.

19. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

header information; and
file icon.

20. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file content; and
file icon.

21. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file name extension; and
file icon.

22. (Original) A method for detecting malicious content according to claim 1 and wherein said at least two characteristics comprise:

file name extension; and
file content.

23. (Currently Amended) A method of detecting malicious content comprising:

obtaining information relating to at least two different corresponding characteristics of a digital object;

analyzing said information to categorize said digital object into at least two categories;

comparing said at least two categories to decide whether there exists a mismatch therebetween;

upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

24. (Original) A method for detecting malicious content according to claim 23 and wherein said malicious content comprises malicious code.

25. (Original) A method for detecting malicious content according to claim 23 and wherein said malicious content comprises masqueraded content.

26. (Original) A method for detecting malicious content according to claim 23 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

27. (Original) A method for detecting malicious content according to claim 26 and wherein said malicious content comprises malicious code.

28. (Original) A method for detecting malicious content according to claim 26 and wherein said malicious content comprises masqueraded content.

29. (Original) A method for detecting malicious content according to claim 23 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

30. (Original) A method for detecting malicious content according to claim 29 and wherein said malicious content comprises malicious code.

31. (Original) A method for detecting malicious content according to claim 29 and wherein said malicious content comprises masqueraded content.

32. (Original) A method for detecting malicious content according to claim 29 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

33. (Original) A method for detecting malicious content according to claim 32 and wherein said malicious content comprises malicious code.

34. (Original) A method for detecting malicious content according to claim 32 and wherein said malicious content comprises masqueraded content.

35. (Original) A method for detecting malicious content according to claim 23 and wherein said digital object comprises a file.

36. (Original) A method for detecting malicious content according to claim 23 and wherein said digital object comprises an e-mail attachment.

37. (Original) A method for detecting malicious content according to claim 23 and wherein said digital object comprises a web page.

38. (Original) A method for detecting malicious content according to claim 23 and wherein said digital object comprises a storage medium.

39. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and
file content.

40. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and
file name extension.

41. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

header information; and
file icon.

42. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file content; and
file icon.

43. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file name extension; and
file icon.

44. (Original) A method for detecting malicious content according to claim 23 and wherein said at least two characteristics comprise:

file name extension; and
file content.

45. (Currently Amended) A method of detecting malicious content comprising:

examining at least two different corresponding characteristics of a digital object, each of which characteristics may be selected by a creator of the digital object independently of selection of another characteristic;

analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

46. (Original) A method for detecting malicious content according to claim 45 and wherein said malicious content comprises malicious code.

47. (Original) A method for detecting malicious content according to claim 45 and wherein said malicious content comprises masqueraded content.

48. (Original) A method for detecting malicious content according to claim 45 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

49. (Original) A method for detecting malicious content according to claim 48 and wherein said malicious content comprises malicious code.

50. (Original) A method for detecting malicious content according to claim 48 and wherein said malicious content comprises masqueraded content.

51. (Original) A method for detecting malicious content according to claim 45 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

52. (Original) A method for detecting malicious content according to claim 51 and wherein said malicious content comprises malicious code.

53. (Original) A method for detecting malicious content according to claim 51 and wherein said malicious content comprises masqueraded content.

54. (Original) A method for detecting malicious content according to claim 51 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

55. (Original) A method for detecting malicious content according to claim 54 and wherein said malicious content comprises malicious code.

56. (Original) A method for detecting malicious content according to claim 54 and wherein said malicious content comprises masqueraded content.

57. (Original) A method for detecting malicious content according to claim 45 and wherein said digital object comprises a file.

58. (Original) A method for detecting malicious content according to claim 45 and wherein said digital object comprises an e-mail attachment.

59. (Original) A method for detecting malicious content according to claim 45 and wherein said digital object comprises a web page.

60. (Original) A method for detecting malicious content according to claim 45 and wherein said digital object comprises a storage medium.

61. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and
file content.

62. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and
file name extension.

63. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

header information; and
file icon.

64. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file content; and
file icon.

65. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file name extension; and
file icon.

66. (Original) A method for detecting malicious content according to claim 45 and wherein said at least two characteristics comprise:

file name extension; and
file content.

67. (Currently Amended) A system for detecting malicious content comprising:

a digital object examiner, examining at least two different corresponding characteristics of a digital object;

a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and

a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

68. (Original) A system for detecting malicious content according to claim 67 and wherein said malicious content comprises malicious code.

69. (Original) A system for detecting malicious content according to claim 67 and wherein said malicious content comprises masqueraded content.

70. (Original) A system for detecting malicious content according to claim 67 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and

file icon.

71. (Original) A system for detecting malicious content according to claim 70 and wherein said malicious content comprises malicious code.

72. (Original) A system for detecting malicious content according to claim 70 and wherein said malicious content comprises masqueraded content.

73. (Original) A system for detecting malicious content according to claim 67 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

74. (Original) A system for detecting malicious content according to claim 73 and wherein said malicious content comprises malicious code.

75. (Original) A system for detecting malicious content according to claim 73 and wherein said malicious content comprises masqueraded content.

76. (Original) A system for detecting malicious content according to claim 73 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

77. (Original) A system for detecting malicious content according to claim 76 and wherein said malicious content comprises malicious code.

78. (Original) A system for detecting malicious content according to claim 76 and wherein said malicious content comprises masqueraded content.

79. (Original) A system for detecting malicious content according to claim 67 and wherein said digital object comprises a file.

80. (Original) A system for detecting malicious content according to claim 67 and wherein said digital object comprises an e-mail attachment.

81. (Original) A system for detecting malicious content according to claim 67 and wherein said digital object comprises a web page.

82. (Original) A system for detecting malicious content according to claim 67 and wherein said digital object comprises a storage medium.

83. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and
file content.

84. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and
file name extension.

85. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

header information; and
file icon.

86. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file content; and
file icon.

87. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file name extension; and
file icon.

88. (Original) A system for detecting malicious content according to claim 67 and wherein said at least two characteristics comprise:

file name extension; and
file content.

89. (Withdrawn) A system according to claim 67 and wherein:

said digital object examiner comprises a digital object examiner server subsystem;

said characteristics mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

90. (Withdrawn) A system for detecting malicious content according to claim 89 and wherein said malicious content comprises malicious code.

91. (Withdrawn) A system for detecting malicious content according to claim 89 and wherein said malicious content comprises masqueraded content.

92. (Withdrawn) A system for detecting malicious content according to claim 89 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;

file name extension; and
file icon.

93. (Withdrawn) A system for detecting malicious content according to claim 92 and wherein said malicious content comprises malicious code.

94. (Withdrawn) A system for detecting malicious content according to claim 92 and wherein said malicious content comprises masqueraded content.

95. (Withdrawn) A system for detecting malicious content according to claim 89 and wherein said digital object is selected from a set consisting of:

a file;
an e-mail attachment;
a web page; and
a storage medium.

96. (Withdrawn) A system for detecting malicious content according to claim 95 and wherein said malicious content comprises malicious code.

97. (Withdrawn) A system for detecting malicious content according to claim 95 and wherein said malicious content comprises masqueraded content.

98. (Withdrawn) A system for detecting malicious content according to claim 95 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

99. (Withdrawn) A system for detecting malicious content according to claim 98 and wherein said malicious content comprises malicious code.

100. (Withdrawn) A system for detecting malicious content according to claim 98 and wherein said malicious content comprises masqueraded content.

101. (Withdrawn) A system according to claim 67 and wherein:
said digital object examiner comprises a digital object examiner client subsystem;
said characteristics mismatch detector comprising a mismatch detector client subsystem; and
said digital object classifier comprising a mismatch detector client subsystem.

102. (Withdrawn) A system for detecting malicious content according to claim 101 and wherein said malicious content comprises malicious code.

103. (Withdrawn) A system for detecting malicious content according to claim 101 and wherein said malicious content comprises masqueraded content.

104. (Withdrawn) A system for detecting malicious content according to claim 101 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

105. (Withdrawn) A system for detecting malicious content according to claim 104 and wherein said malicious content comprises malicious code.

106. (Withdrawn) A system for detecting malicious content according to claim 105 and wherein said malicious content comprises masqueraded content.

107. (Withdrawn) A system for detecting malicious content according to claim 101 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

108. (Withdrawn) A system for detecting malicious content according to claim 107 and wherein said malicious content comprises malicious code.

109. (Withdrawn) A system for detecting malicious content according to claim 107 and wherein said malicious content comprises masqueraded content.

110. (Withdrawn) A system for detecting malicious content according to claim 107 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

111. (Withdrawn) A system for detecting malicious content according to claim 110 and wherein said malicious content comprises malicious code.

112. (Withdrawn) A system for detecting malicious content according to claim 110 and wherein said malicious content comprises masqueraded content.

113. (Original) A system according to claim 67 and wherein:

- said digital object examiner comprises a digital object examiner gateway subsystem;
- said characteristics mismatch detector comprising a mismatch detector gateway subsystem; and

said digital object classifier comprising a mismatch detector gateway subsystem.

114. (Original) A system for detecting malicious content according to claim 113 and wherein said malicious content comprises malicious code.

115. (Original) A system for detecting malicious content according to claim 113 and wherein said malicious content comprises masqueraded content.

116. (Original) A system for detecting malicious content according to claim 113 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

117. (Original) A system for detecting malicious content according to claim 116 and wherein said malicious content comprises malicious code.

118. (Original) A system for detecting malicious content according to claim 116 and wherein said malicious content comprises masqueraded content.

119. (Original) A system for detecting malicious content according to claim 113 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

120. (Original) A system for detecting malicious content according to claim 119 and wherein said malicious content comprises malicious code.

121. (Original) A system for detecting malicious content according to claim 119 and wherein said malicious content comprises masqueraded content.

122. (Original) A system for detecting malicious content according to claim 119 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

123. (Original) A system for detecting malicious content according to claim 122 and wherein said malicious content comprises malicious code.

124. (Original) A system for detecting malicious content according to claim 122 and wherein said malicious content comprises masqueraded content.

125. (Original) A system according to claim 67 and wherein:

- said digital object examiner is selected from a set consisting of:

- a digital object examiner server subsystem;
 - a digital object examiner client subsystem;
 - a digital object examiner gateway subsystem;

- said digital characteristics mismatch detector is selected from a set consisting of:

- a characteristics mismatch detector server subsystem;
 - a characteristics mismatch detector client subsystem;
 - a characteristics mismatch detector gateway subsystem;

- and

- said digital object classifier is selected from a set consisting of:

- a digital object classifier server subsystem;
 - a digital object classifier client subsystem;

a digital object classifier gateway subsystem.

126. (Currently Amended) A system for detecting malicious content comprising:

a digital object information obtainer, obtaining information related to at least two different corresponding characteristics of a digital object;

a characteristic based categorizer, categorizing said information into at least two categories;

a categories mismatch detector, analyzing said at least two categories to determine whether there exists a mismatch therebetween; and

a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

127. (Original) A system for detecting malicious content according to claim 126 and wherein said malicious content comprises malicious code.

128. (Original) A system for detecting malicious content according to claim 126 and wherein said malicious content comprises masqueraded content.

129. (Original) A system for detecting malicious content according to claim 126 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

130. (Original) A system for detecting malicious content according to claim 129 and wherein said malicious content comprises malicious code.

131. (Original) A system for detecting malicious content according to claim 129 and wherein said malicious content comprises masqueraded content.

132. (Original) A system for detecting malicious content according to claim 126 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

133. (Original) A system for detecting malicious content according to claim 132 and wherein said malicious content comprises malicious code.

134. (Original) A system for detecting malicious content according to claim 132 and wherein said malicious content comprises masqueraded content.

135. (Original) A system for detecting malicious content according to claim 132 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

136. (Original) A system for detecting malicious content according to claim 135 and wherein said malicious content comprises malicious code.

137. (Original) A system for detecting malicious content according to claim 135 and wherein said malicious content comprises masqueraded content.

138. (Original) A system for detecting malicious content according to claim 126 and wherein said digital object comprises a file.

139. (Original) A system for detecting malicious content according to claim 126 and wherein said digital object comprises an e-mail attachment.

140. (Original) A system for detecting malicious content according to claim 126 and wherein said digital object comprises a web page.

141. (Original) A system for detecting malicious content according to claim 126 and wherein said digital object comprises a storage medium.

142. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and
file content.

143. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and
file name extension.

144. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

header information; and
file icon.

145. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file content; and
file icon.

146. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file name extension; and

file icon.

147. (Original) A system for detecting malicious content according to claim 126 and wherein said at least two characteristics comprise:

file name extension; and
file content.

148. (Withdrawn) A system according to claim 126 and wherein:

said digital object information obtainer comprises a digital object information obtainer server subsystem;

said characteristic based categorizer comprises a characteristic based categorizer server subsystem;

said categories mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

149. (Withdrawn) A system for detecting malicious content according to claim 148 and wherein said malicious content comprises malicious code.

150. (Withdrawn) A system for detecting malicious content according to claim 148 and wherein said malicious content comprises masqueraded content.

151. (Withdrawn) A system for detecting malicious content according to claim 148 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

152. (Withdrawn) A system for detecting malicious content according to claim 151 and wherein said malicious content comprises malicious code.

153. (Withdrawn) A system for detecting malicious content according to claim 151 and wherein said malicious content comprises masqueraded content.

154. (Withdrawn) A system for detecting malicious content according to claim 148 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

155. (Withdrawn) A system for detecting malicious content according to claim 154 and wherein said malicious content comprises malicious code.

156. (Withdrawn) A system for detecting malicious content according to claim 154 and wherein said malicious content comprises masqueraded content.

157. (Withdrawn) A system for detecting malicious content according to claim 154 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

158. (Withdrawn) A system for detecting malicious content according to claim 157 and wherein said malicious content comprises malicious code.

159. (Withdrawn) A system for detecting malicious content according to claim 157 and wherein said malicious content comprises masqueraded content.

160. (Withdrawn) A system according to claim 126 and wherein:

said digital object information obtainer comprises a digital object information obtainer client subsystem;

said characteristic based categorizer comprises a characteristic based categorizer client subsystem;

said categories mismatch detector comprising a mismatch detector client subsystem; and

said digital object classifier comprising a mismatch detector client subsystem.

161. (Withdrawn) A system for detecting malicious content according to claim 160 and wherein said malicious content comprises malicious code.

162. (Withdrawn) A system for detecting malicious content according to claim 160 and wherein said malicious content comprises masqueraded content.

163. (Withdrawn) A system for detecting malicious content according to claim 160 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

164. (Withdrawn) A system for detecting malicious content according to claim 163 and wherein said malicious content comprises malicious code.

165. (Withdrawn) A system for detecting malicious content according to claim 164 and wherein said malicious content comprises masqueraded content.

166. (Withdrawn) A system for detecting malicious content according to claim 160 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

167. (Withdrawn) A system for detecting malicious content according to claim 166 and wherein said malicious content comprises malicious code.

168. (Withdrawn) A system for detecting malicious content according to claim 166 and wherein said malicious content comprises masqueraded content.

169. (Withdrawn) A system for detecting malicious content according to claim 166 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

170. (Withdrawn) A system for detecting malicious content according to claim 169 and wherein said malicious content comprises malicious code.

171. (Withdrawn) A system for detecting malicious content according to claim 169 and wherein said malicious content comprises masqueraded content.

172. (Original) A system according to claim 126 and wherein:

- said digital object information obtainer comprises a digital object information obtainer gateway subsystem;
- said characteristic based categorizer comprises a characteristic based categorizer gateway subsystem;

said categories mismatch detector comprising a mismatch detector gateway subsystem; and

said digital object classifier comprising a mismatch detector gateway subsystem.

173. (Original) A system for detecting malicious content according to claim 172 and wherein said malicious content comprises malicious code.

174. (Original) A system for detecting malicious content according to claim 172 and wherein said malicious content comprises masqueraded content.

175. (Original) A system for detecting malicious content according to claim 172 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

176. (Original) A system for detecting malicious content according to claim 175 and wherein said malicious content comprises malicious code.

177. (Original) A system for detecting malicious content according to claim 175 and wherein said malicious content comprises masqueraded content.

178. (Original) A system for detecting malicious content according to claim 172 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

179. (Original) A system for detecting malicious content according to claim 178 and wherein said malicious content comprises malicious code.

180. (Original) A system for detecting malicious content according to claim 178 and wherein said malicious content comprises masqueraded content.

181. (Original) A system for detecting malicious content according to claim 178 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

182. (Original) A system for detecting malicious content according to claim 181 and wherein said malicious content comprises malicious code.

183. (Original) A system for detecting malicious content according to claim 181 and wherein said malicious content comprises masqueraded content.

184. (Original) A system according to claim 126 and wherein:
said digital object information obtainer is selected from a set consisting of:

- a digital object information server subsystem;
- a digital object information client subsystem;
- a digital object information gateway subsystem;
- said characteristic based categorizer is selected from a set consisting of:
 - a characteristic based categorizer server subsystem;
 - a characteristic based categorizer client subsystem;
 - a characteristic based categorizer gateway subsystem;
- said categories mismatch detector is selected from a set consisting of:
 - a categories mismatch detector server subsystem;

- a categories mismatch detector client subsystem;
- a categories mismatch detector gateway subsystem;
- and
- said digital object classifier is selected from a set consisting of:
 - a digital object classifier server subsystem;
 - a digital object classifier client subsystem;
 - a digital object classifier gateway subsystem.

185. (Currently Amended) A system for detecting malicious content comprising:

- a digital object examiner, examining at least two different corresponding characteristics of a digital object, each of which characteristics may be selected by a creator of the digital object independently of selection of another characteristic;
- a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and
- a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content.

186. (Original) A system for detecting malicious content according to claim 185 and wherein said malicious content comprises malicious code.

187. (Original) A system for detecting malicious content according to claim 185 and wherein said malicious content comprises masqueraded content.

188. (Original) A system for detecting malicious content according to claim 185 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

189. (Original) A system for detecting malicious content according to claim 188 and wherein said malicious content comprises malicious code.

190. (Original) A system for detecting malicious content according to claim 188 and wherein said malicious content comprises masqueraded content.

191. (Original) A system for detecting malicious content according to claim 185 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

192. (Original) A system for detecting malicious content according to claim 191 and wherein said malicious content comprises malicious code.

193. (Original) A system for detecting malicious content according to claim 191 and wherein said malicious content comprises masqueraded content.

194. (Original) A system for detecting malicious content according to claim 191 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

195. (Original) A system for detecting malicious content according to claim 194 and wherein said malicious content comprises malicious code.

196. (Original) A system for detecting malicious content according to claim 194 and wherein said malicious content comprises masqueraded content.

197. (Original) A system for detecting malicious content according to claim 185 and wherein said digital object comprises a file.

198. (Original) A system for detecting malicious content according to claim 185 and wherein said digital object comprises an e-mail attachment.

199. (Original) A system for detecting malicious content according to claim 185 and wherein said digital object comprises a web page.

200. (Original) A system for detecting malicious content according to claim 185 and wherein said digital object comprises a storage medium.

201. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and
file content.

202. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and
file name extension.

203. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

header information; and
file icon.

204. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file content; and
file icon.

205. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file name extension; and
file icon.

206. (Original) A system for detecting malicious content according to claim 185 and wherein said at least two characteristics comprise:

file name extension; and
file content.

207. (Withdrawn) A system according to claim 185 and wherein:

said digital object examiner comprises a digital object examiner server subsystem;

said characteristics mismatch detector comprising a mismatch detector server subsystem; and

said digital object classifier comprising a mismatch detector server subsystem.

208. (Withdrawn) A system for detecting malicious content according to claim 207 and wherein said malicious content comprises malicious code.

209. (Withdrawn) A system for detecting malicious content according to claim 207 and wherein said malicious content comprises masqueraded content.

210. (Withdrawn) A system for detecting malicious content according to claim 207 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;
file content;
file name extension; and
file icon.

211. (Withdrawn) A system for detecting malicious content according to claim 210 and wherein said malicious content comprises malicious code.

212. (Withdrawn) A system for detecting malicious content according to claim 210 and wherein said malicious content comprises masqueraded content.

213. (Withdrawn) A system for detecting malicious content according to claim 207 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

214. (Withdrawn) A system for detecting malicious content according to claim 213 and wherein said malicious content comprises malicious code.

215. (Withdrawn) A system for detecting malicious content according to claim 213 and wherein said malicious content comprises masqueraded content.

216. (Withdrawn) A system for detecting malicious content according to claim 213 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

217. (Withdrawn) A system for detecting malicious content according to claim 216 and wherein said malicious content comprises malicious code.

218. (Withdrawn) A system for detecting malicious content according to claim 216 and wherein said malicious content comprises masqueraded content.

219. (Withdrawn) A system according to claim 185 and wherein:

said digital object examiner comprises a digital object examiner client subsystem;

said characteristics mismatch detector comprising a mismatch detector client subsystem; and

said digital object classifier comprising a mismatch detector client subsystem.

220. (Withdrawn) A system for detecting malicious content according to claim 219 and wherein said malicious content comprises malicious code.

221. (Withdrawn) A system for detecting malicious content according to claim 219 and wherein said malicious content comprises masqueraded content.

222. (Withdrawn) A system for detecting malicious content according to claim 219 and wherein at least one of said at least two characteristics is selected from a set consisting of:

header information;

file content;

file name extension; and

file icon.

223. (Withdrawn) A system for detecting malicious content according to claim 222 and wherein said malicious content comprises malicious code.

224. (Withdrawn) A system for detecting malicious content according to claim 223 and wherein said malicious content comprises masqueraded content.

225. (Withdrawn) A system for detecting malicious content according to claim 219 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

226. (Withdrawn) A system for detecting malicious content according to claim 225 and wherein said malicious content comprises malicious code.

227. (Withdrawn) A system for detecting malicious content according to claim 225 and wherein said malicious content comprises masqueraded content.

228. (Withdrawn) A system for detecting malicious content according to claim 225 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

229. (Withdrawn) A system for detecting malicious content according to claim 228 and wherein said malicious content comprises malicious code.

230. (Withdrawn) A system for detecting malicious content according to claim 228 and wherein said malicious content comprises masqueraded content.

231. (Original) A system according to claim 185 and wherein:

- said digital object examiner comprises a digital object examiner gateway subsystem;
- said characteristics mismatch detector comprising a mismatch detector gateway subsystem; and

said digital object classifier comprising a mismatch detector gateway subsystem.

232. (Original) A system for detecting malicious content according to claim 231 and wherein said malicious content comprises malicious code.

233. (Original) A system for detecting malicious content according to claim 231 and wherein said malicious content comprises masqueraded content.

234. (Original) A system for detecting malicious content according to claim 231 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

235. (Original) A system for detecting malicious content according to claim 234 and wherein said malicious content comprises malicious code.

236. (Original) A system for detecting malicious content according to claim 234 and wherein said malicious content comprises masqueraded content.

237. (Original) A system for detecting malicious content according to claim 231 and wherein said digital object is selected from a set consisting of:

- a file;
- an e-mail attachment;
- a web page; and
- a storage medium.

238. (Original) A system for detecting malicious content according to claim 237 and wherein said malicious content comprises malicious code.

239. (Original) A system for detecting malicious content according to claim 237 and wherein said malicious content comprises masqueraded content.

240. (Original) A system for detecting malicious content according to claim 237 and wherein at least one of said at least two characteristics is selected from a set consisting of:

- header information;
- file content;
- file name extension; and
- file icon.

241. (Original) A system for detecting malicious content according to claim 240 and wherein said malicious content comprises malicious code.

242. (Original) A system for detecting malicious content according to claim 240 and wherein said malicious content comprises masqueraded content.

243. (Original) A system according to claim 185 and wherein:

- said digital object examiner is selected from a set consisting of:

- a digital object examiner server subsystem;
 - a digital object examiner client subsystem;
 - a digital object examiner gateway subsystem;

- said digital characteristics mismatch detector is selected from a set consisting of:

- a characteristics mismatch detector server subsystem;
 - a characteristics mismatch detector client subsystem;
 - a characteristics mismatch detector gateway subsystem;

and

said digital object classifier is selected from a set consisting of:

- a digital object classifier server subsystem;
- a digital object classifier client subsystem;
- a digital object classifier gateway subsystem.